

Fig. 1

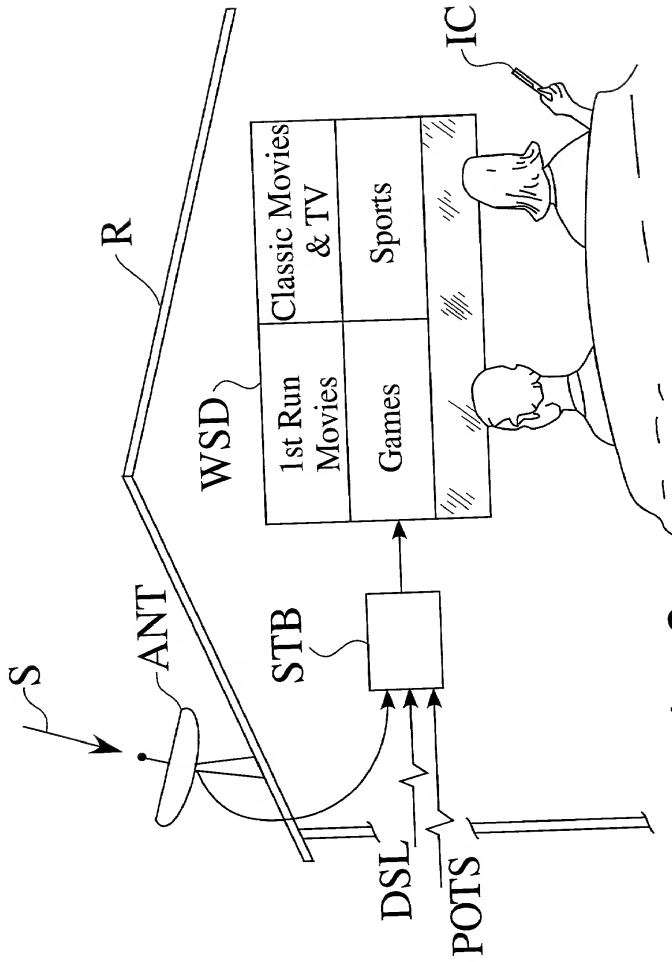


Fig. 2

3/21

Sky Vault Operation Flow Chart

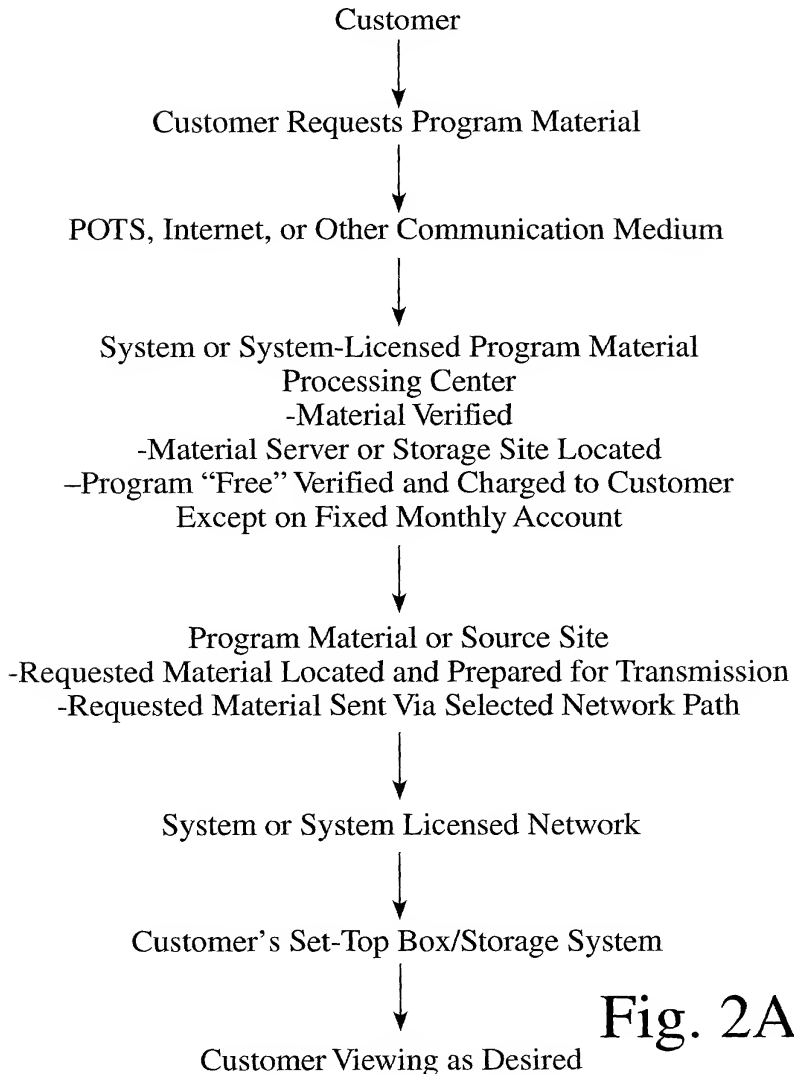


Fig. 2A

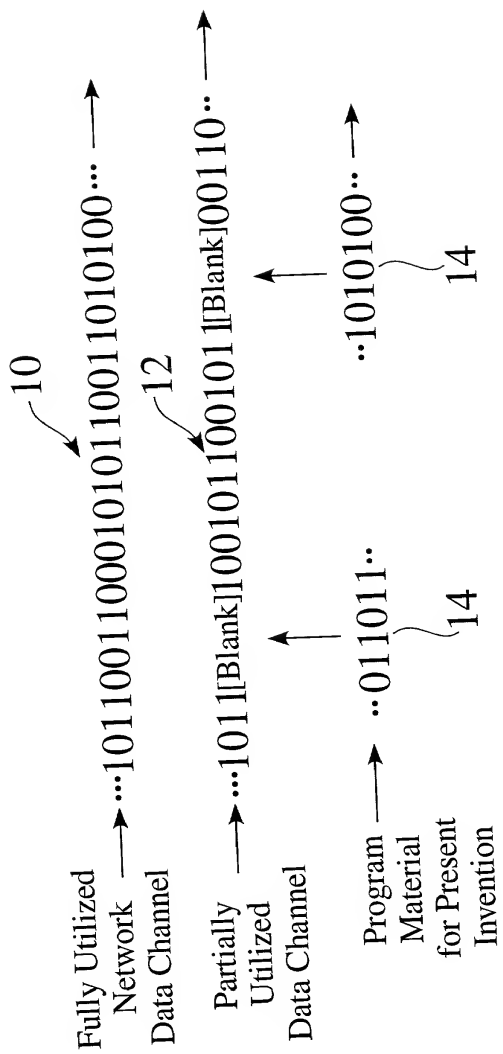


Fig. 3

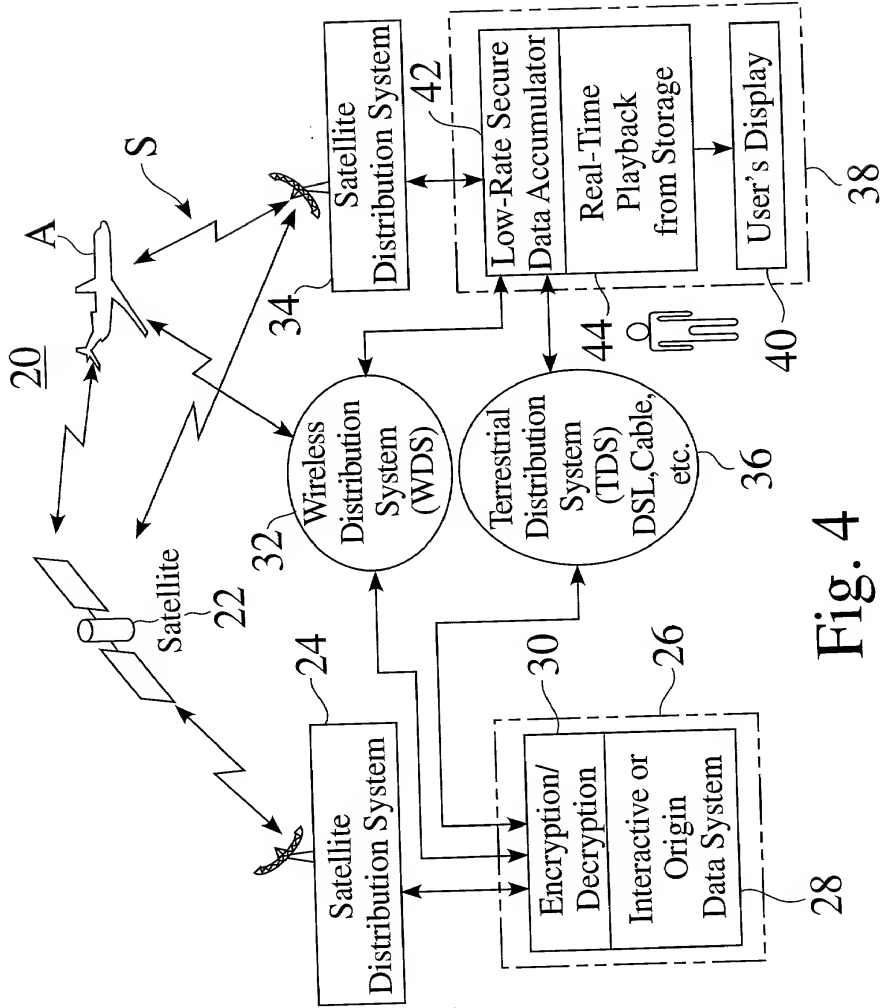
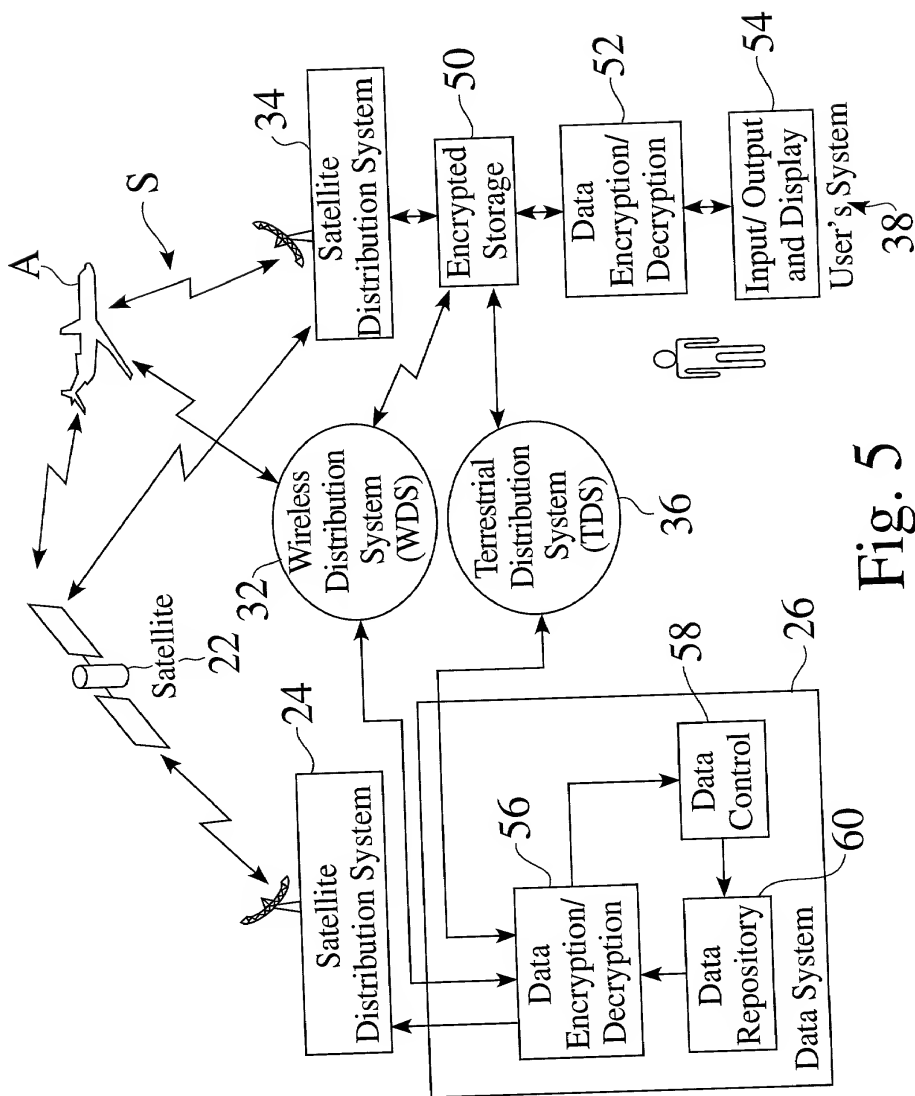


Fig. 4



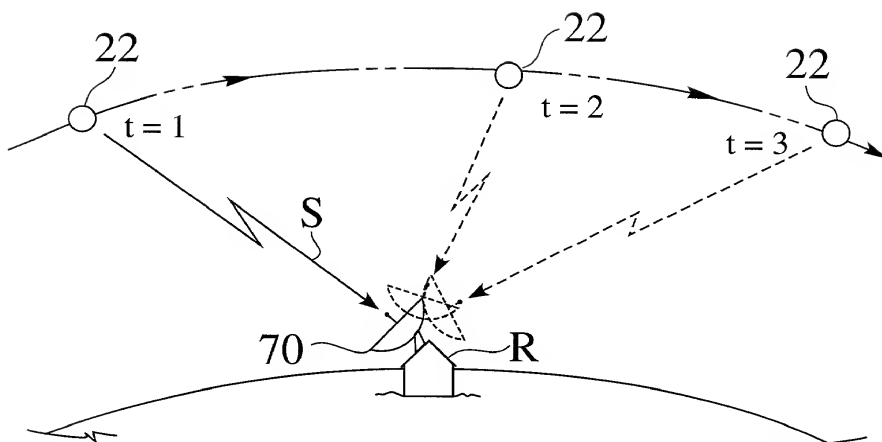


Fig. 6

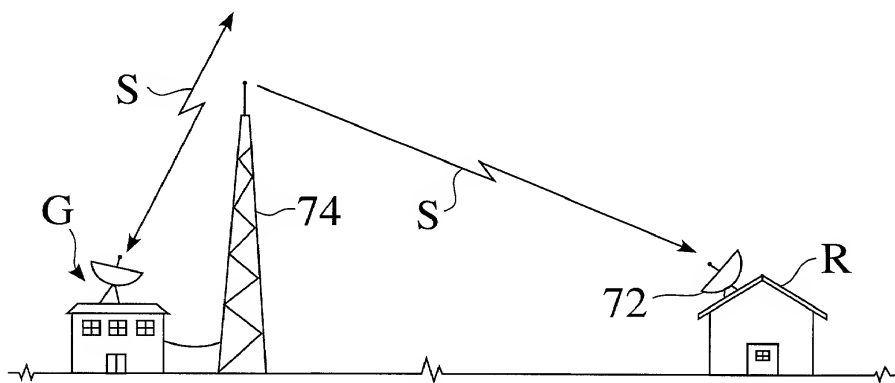


Fig. 7

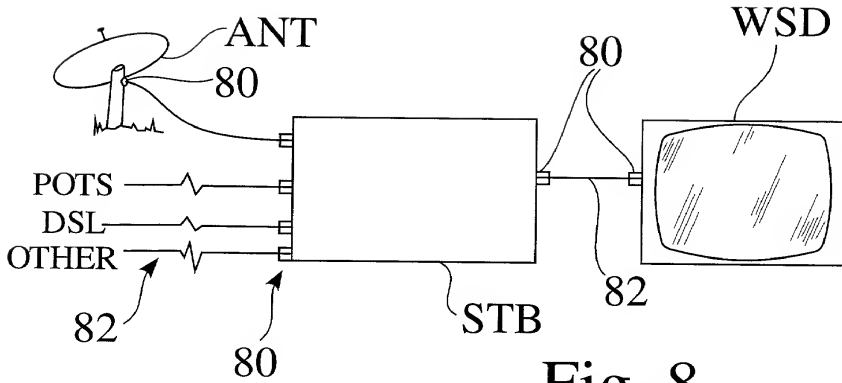


Fig. 8

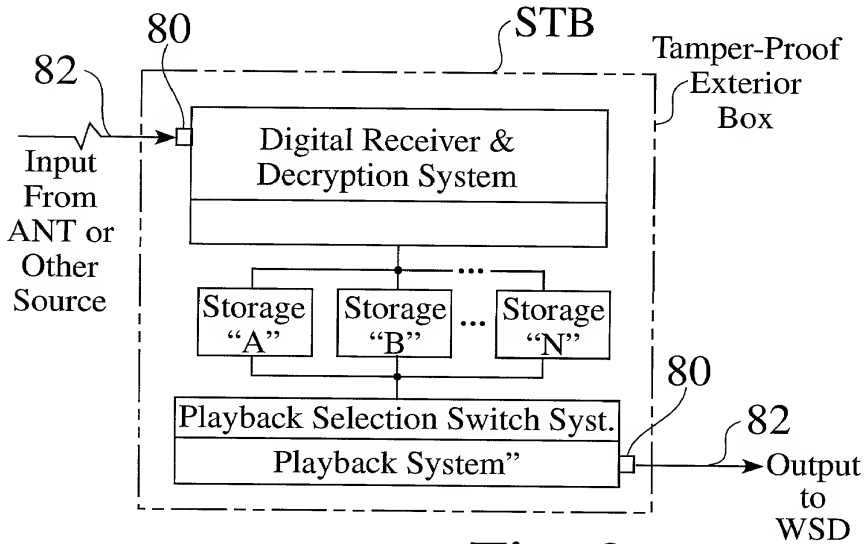


Fig. 9



9/21

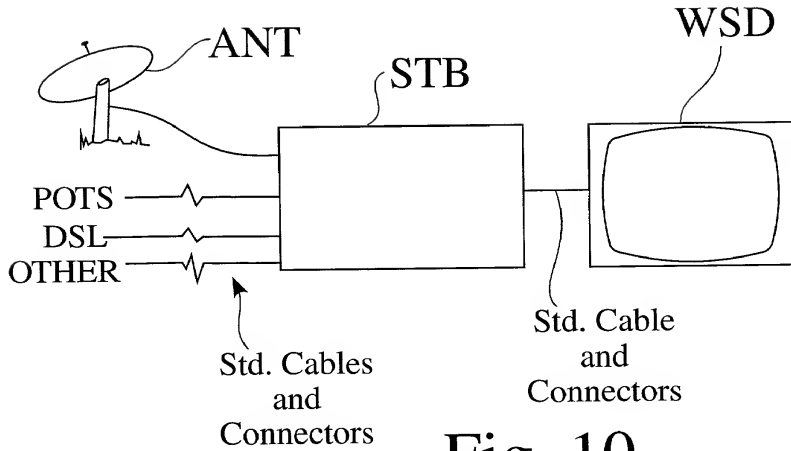


Fig. 10

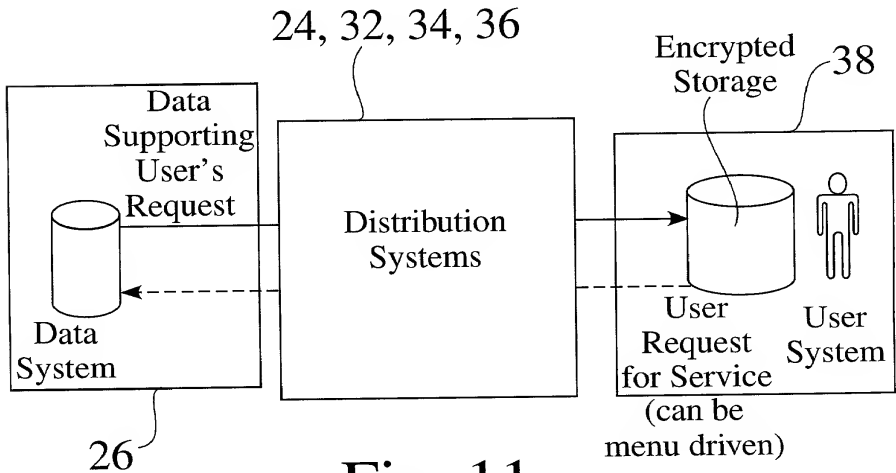


Fig. 11

10/21

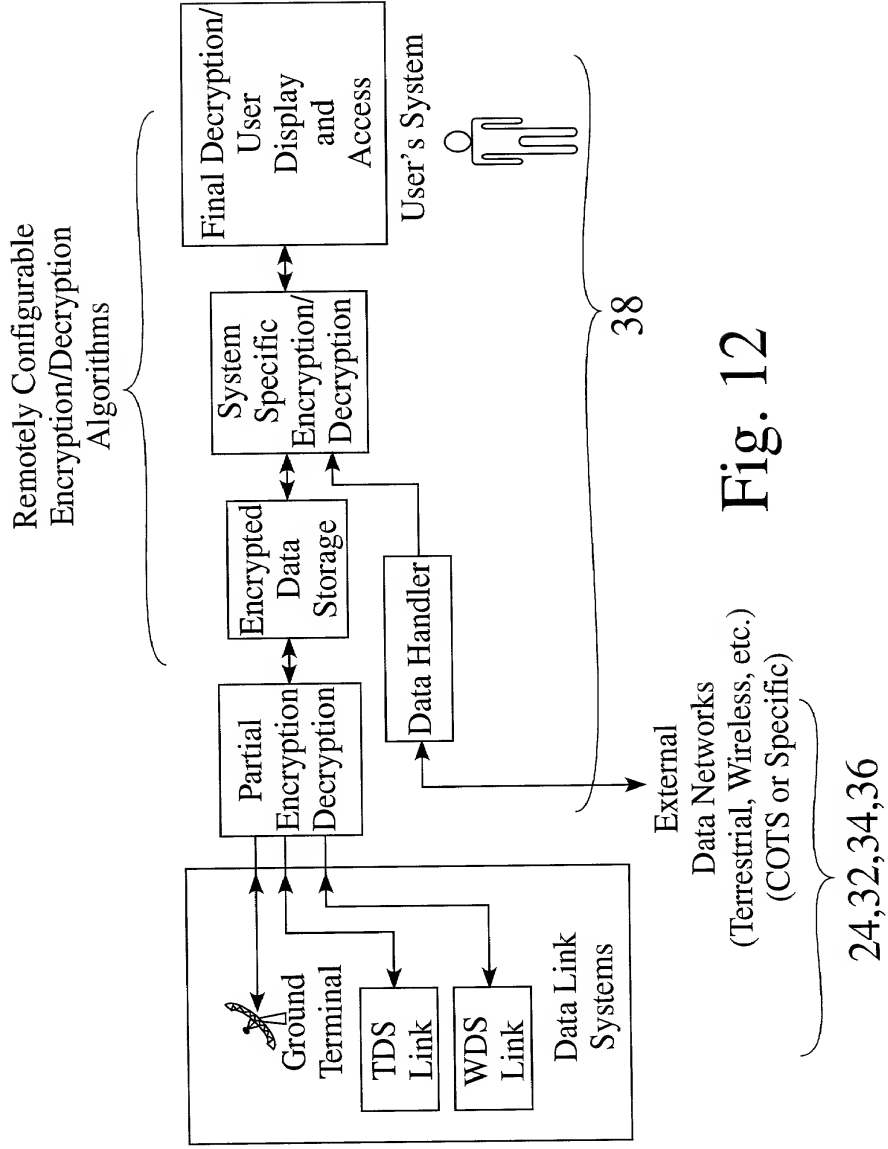


Fig. 12

Decrypted Data will  
Drive ONLY this  
User Display

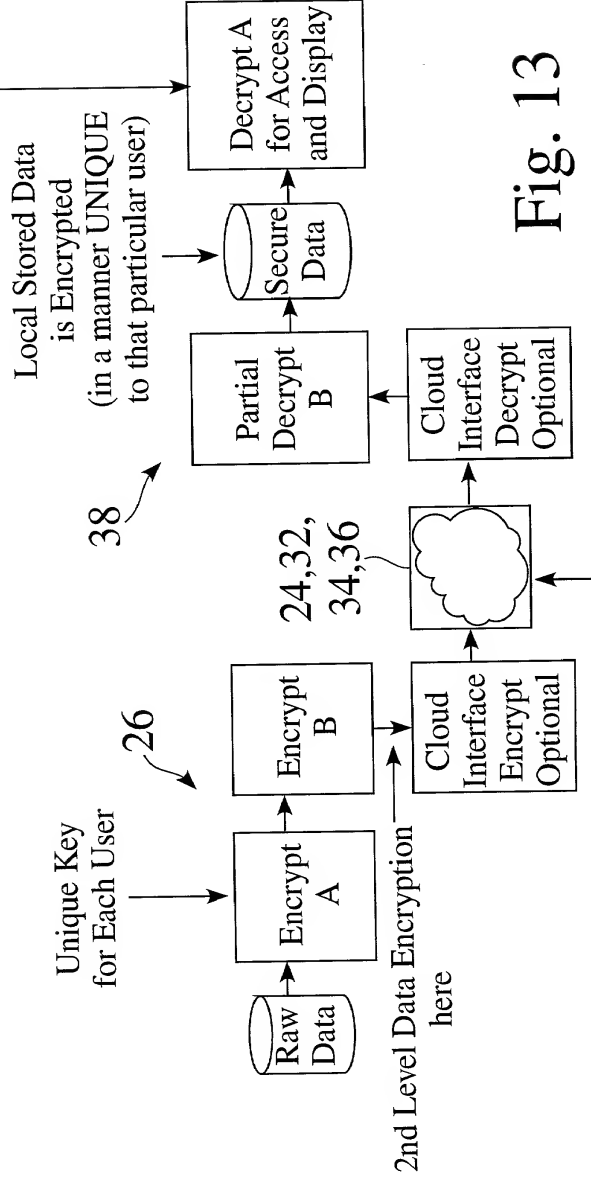


Fig. 13

12/21

### System Server Functions

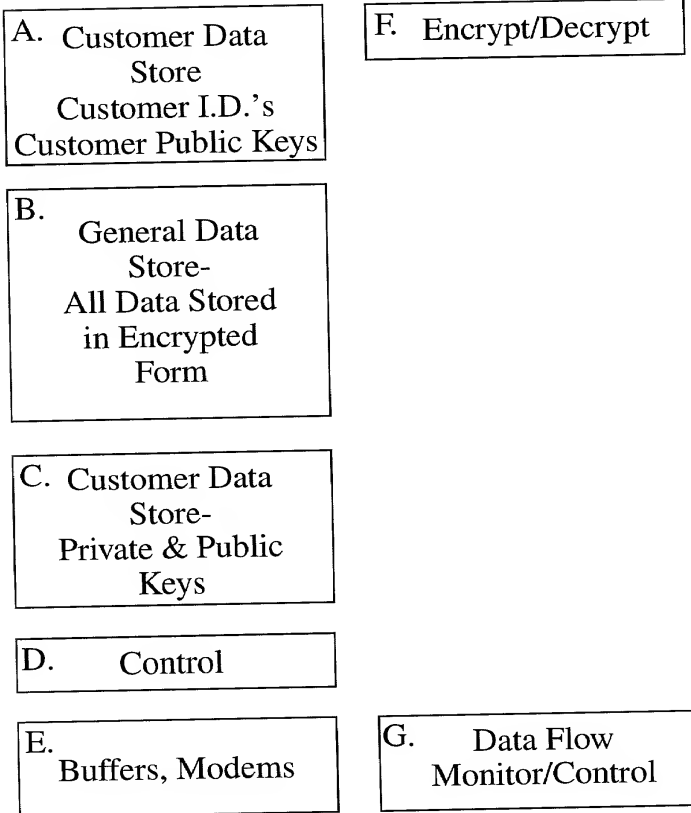
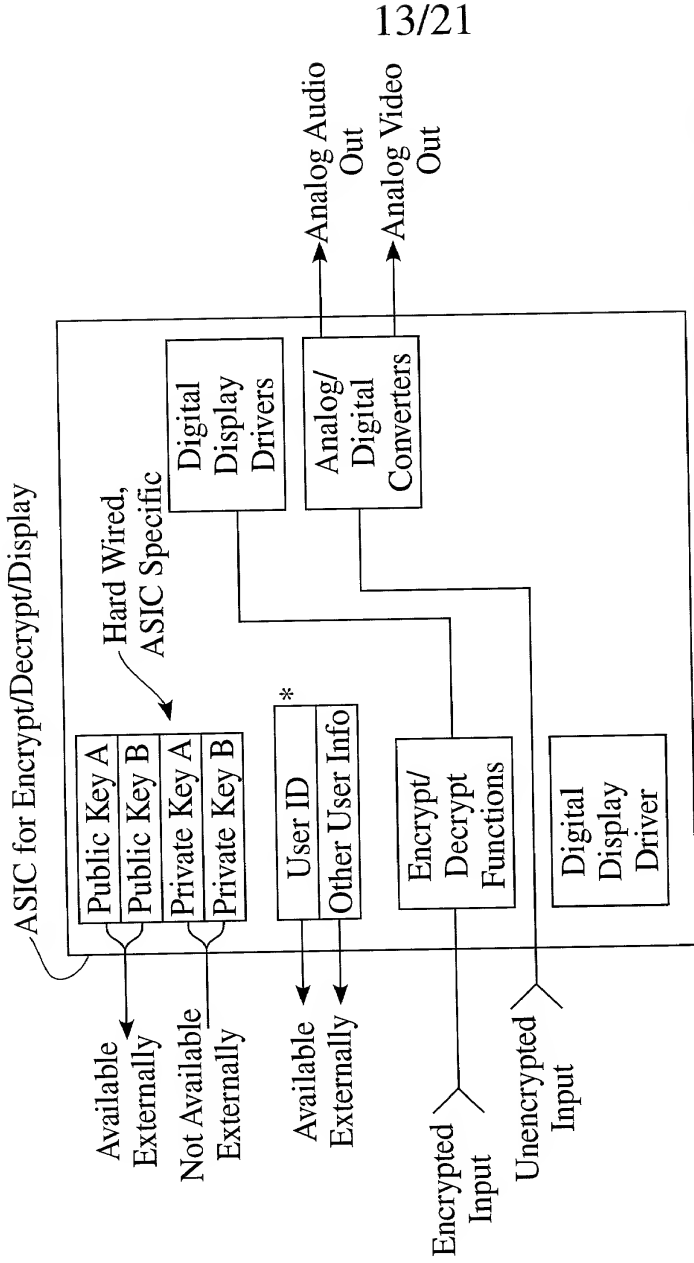


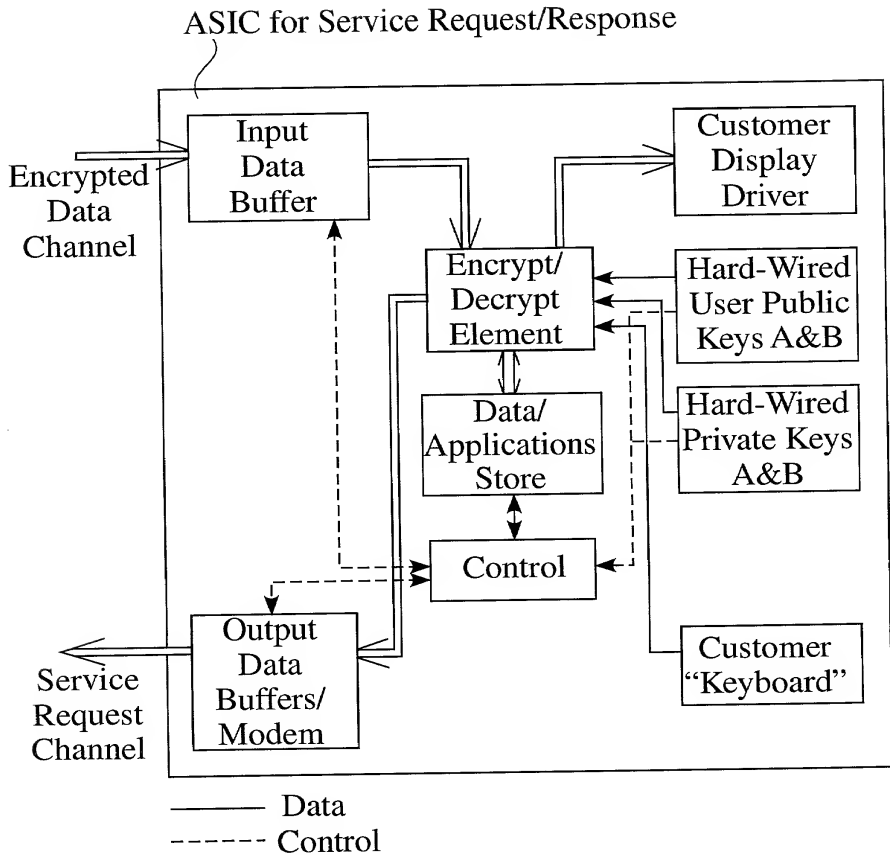
Fig. 14



\* May Be Stored Externally

Notes: 1) Customer-Specific ASIC, Analog & Digital Circuits  
2) No Digital, Decrypted Data Available External to ASIC

Fig. 15



Notes: 1) Request for Data - Control sends Public Keys A&B to System Sources via Output Data Buffer; sends Data I.D. Number to identify stored data upon receipt.  
 2) Data Reception - Control identifies Data & applies Private Keys A or B for Storage or Display.

Fig. 16

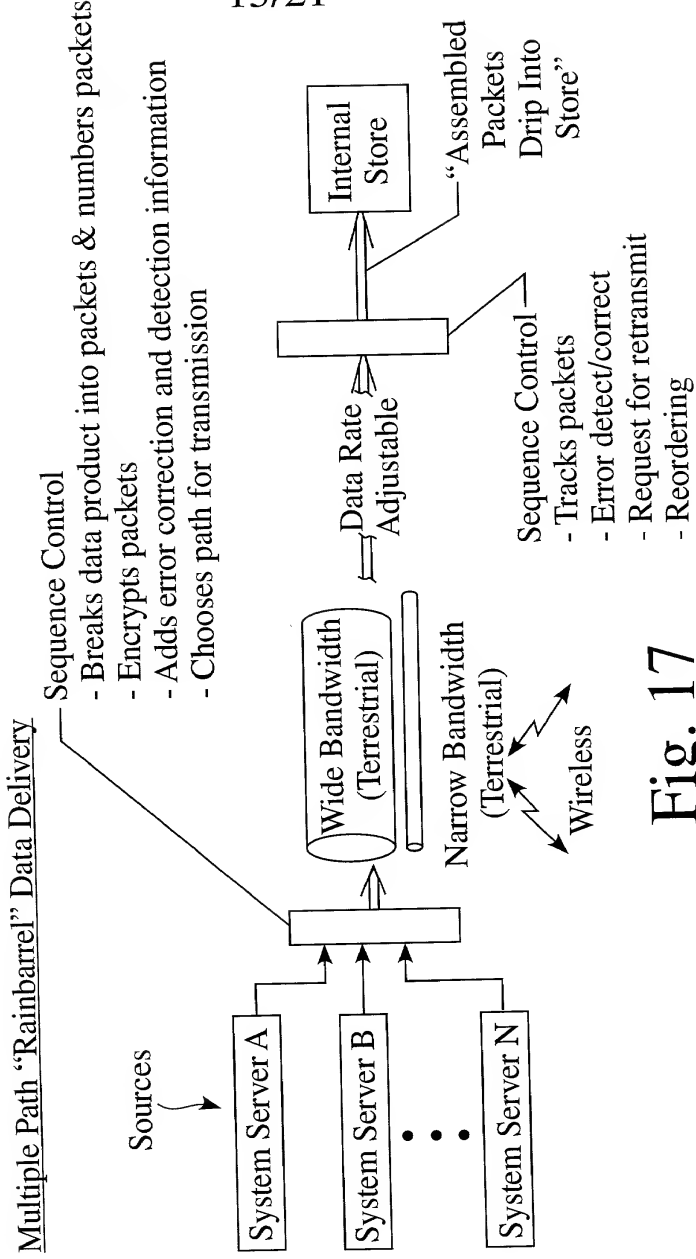


Fig. 17

### Request for Data and Response

- 1) Customer requests data menu from system server.
- 2) System server responds with menu, etc.
- 3) Customer requests "data".
  - Generic request: customer sends customer ID, public key A; encrypts by public key
  - Requests for specific data: customer sends ID, public keys A and B; encrypts by public key
- 4) Network encrypts/decrypts (for example, with https); system server decrypts and searches data base for response.
- 5) System server extracts data, "packetizes" the data.
  - Server encrypts the data with public key A
  - Network encrypts/decrypts
- 6) Network operating system routes encrypted packages over available routes to customer.
- 7) Customer decrypts with private key A
  - Generic request: Display menu
  - Specific request: Data buffered, reassembled and stored in encrypted form.

Fig. 18



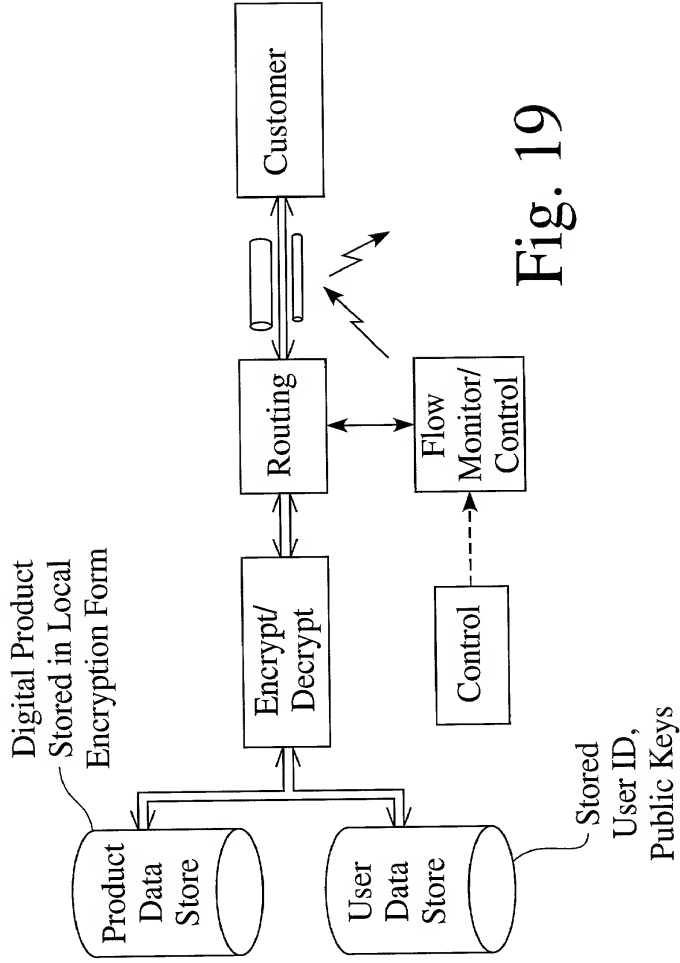
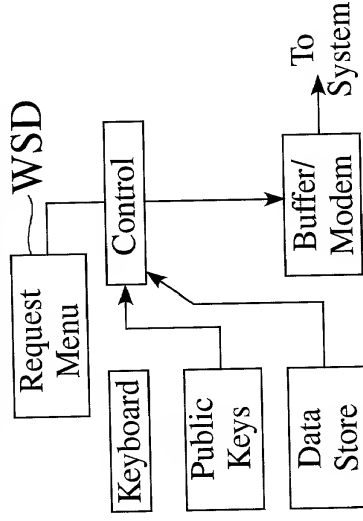


Fig. 19

### User Request for System Menu



- 1) At request for system menu, the following actions occur:
  - Control extracts user ID, public keys A&B from user hardware
  - Control extracts software application containing data request protocols from Data Store and directs request to Output Data Buffer/Modem.
  - Encrypted request is transmitted to a system server via available channel.
  - Additional encryption is available using https when using TCP/IP protocols over the channel.
- 2) At receipt of menu data, Control decrypts with private key B and stores in Data/Application Store.
- 3) When data transfer is complete, Control causes display to indicate "Menu Available."
- 4) Customer requests menu display from the keyboard (or mouse, etc.)
- 5) Control extracts encrypted data from Store and performs second decryption using private key A.
- 6) Data is displayed on screen, but digital unencrypted form of the data is unavailable outside of display ASIC.

**Fig. 20**

### User Request for System Data

- 1) Customer requests system menu data by keyboard (or mouse, etc.)
- 2) Request is encrypted using public key A and stored in Data/Applications Store. Customer ID, public keys A and B are attached.
- 3) Request is also encrypted using System public key and sent to Data Flow Monitor/Control and Buffers/modems for transmission via available digital channel.
- 4) At receipt of data request by System, the following actions occur:
  - Controller stores customer request in a General Data Store.
  - Requested data is encrypted using customer public keys A & B and sent to Data Flow Monitor/Control for progressive transmission through buffers/modems.
  - Selected least significant bits of data, controlled by customer public key, are altered with a **customer-specific** signature.
- 5) When customer receives data, Control decrypts data using private key B and stores blocks in Data/Applications Store. When all data blocks are received, Control notifies user via the display.
- 6) When customer requests to view the data, Control decrypts it using private key A and removes the digital signature. Control then sends the data to the display driver.
- 7) Note that all keys are hardware specific and not available to the operating system. They are usable only by the encrypt/decrypt/display ASIC. No "Hacker" access since digital data is never available outside the user's hardware.

Fig. 21

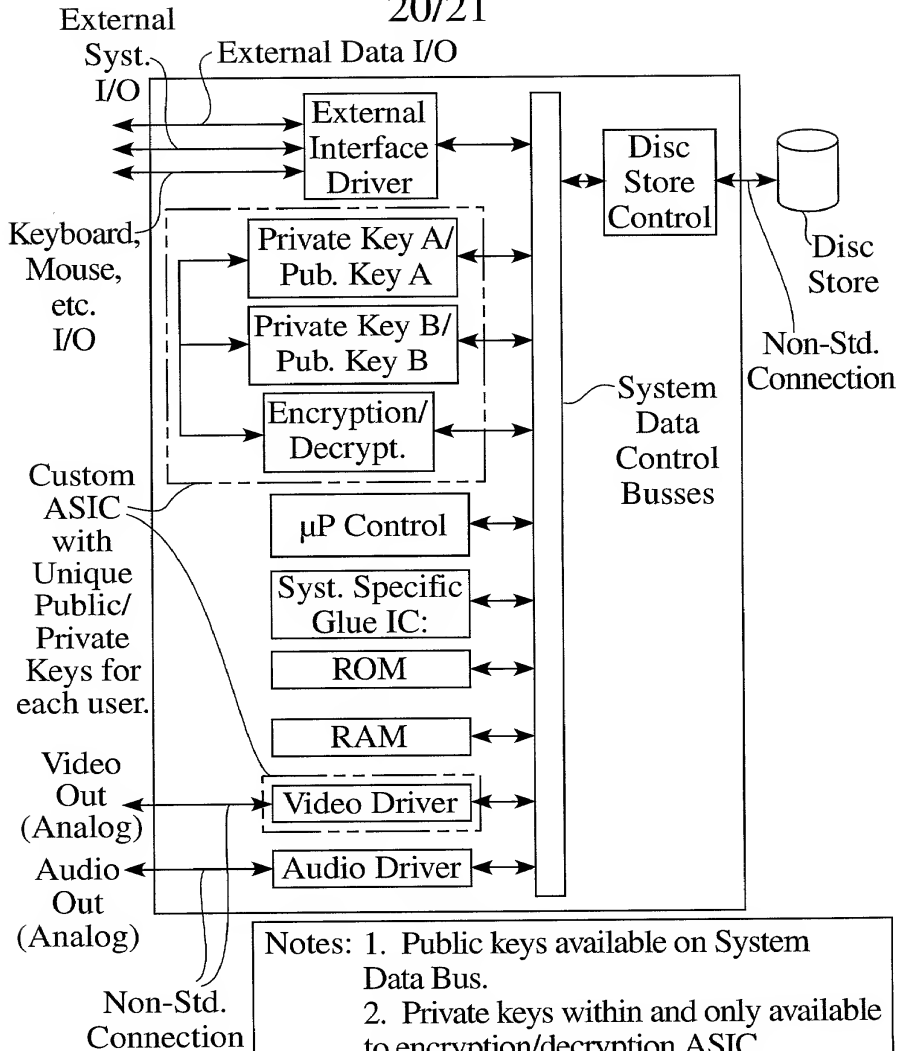


Fig. 22

- Notes:
1. Public keys available on System Data Bus.
  2. Private keys within and only available to encryption/decryption ASIC.
  3. Digital data never available outside of ASIC in unencrypted form.
  4. All data stored on disc, or equivalent, is in encrypted form.
  5. Analog video and audio data transmitted to off-board displays via non-standard connectors and cables.

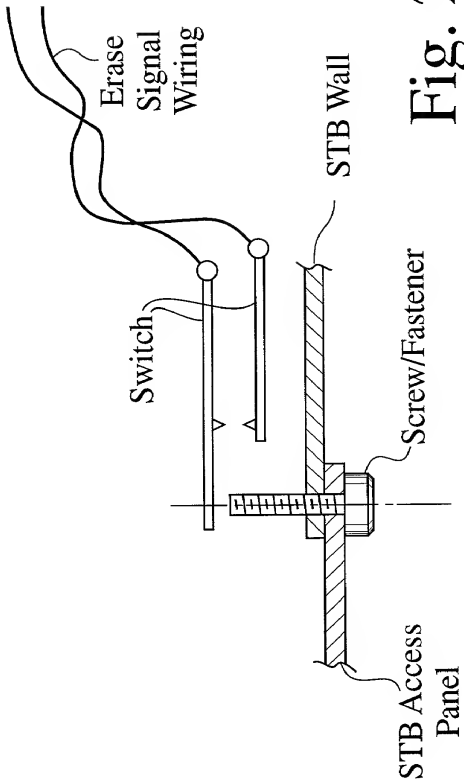


Fig. 23